



Brüssel, den 24. November 2014
(OR. en)

15701/1/14
REV 1

JAI 897
DAPIX 175
CRIMORG 109
ENFOPOL 372

I/A-PUNKT-VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Nr. Vordok.:	11153/2/14 REV 2
Betr.:	Entwurf von Schlussfolgerungen des Rates zu einer aktualisierten Strategie für das Informationsmanagement (IMS) für die innere Sicherheit in der EU

1. Der Rat hat am 30. November 2009 Schlussfolgerungen zu einer Strategie für das Informationsmanagement (IMS) im Bereich der inneren Sicherheit in der EU angenommen ¹. Die Strategie selbst ist langfristig angelegt und kann im Zuge der Weiterentwicklung der übergeordneten Zielvorstellungen weiter ausgestaltet und aktualisiert werden. Daher wurde die Strategie 2009 mit der Maßgabe gebilligt, dass sie bis Ende 2014 überprüft werden sollte.
2. Mit der IMS soll das Informationsmanagement, das für die Durchführung eines zweckdienlichen grenzüberschreitenden Informationsaustauschs zwischen den mit Strafsachen befassten Strafverfolgungs-, Grenzschutz- und Justizbehörden erforderlich ist, unterstützt, gestrafft und erleichtert werden. Die IMS enthält Leitlinien für eine strukturierte und inhaltsorientierte Wiedergabe des in der Praxis bestehenden Bedarfs und gab für eine Reihe von Schwerpunktbereichen die zu erreichenden strategischen Ziele vor.

¹ Dok. 16637/09 JAI 873 CATS 131 ASIM 137 JUSTCIV 249 JURINFO 145.

3. Ergänzt wurde die Strategie durch einen Maßnahmenkatalog/Fahrplan, in dem die konkreten Ziele, Verfahren, Aufgaben und Fristen festgelegt sind. Bisher sind drei Maßnahmenkataloge, jeweils mit einer Laufzeit von 18 Monaten, erstellt worden. Im zweiten Zwischenbericht über die Umsetzung der IMS-Maßnahmenkataloge² werden die Ziele und die bisherigen Ergebnisse kurz erläutert.
4. Die Gruppe "Informationsaustausch und Datenschutz" hat sich in ihren Sitzungen vom 1. Juli und 23. September mit der Bewertung und der Überprüfung der Strategie befasst. Die Delegationen empfahlen, genau zwischen der Strategie als solcher, der Umsetzung auf nationaler oder auf Unionsebene und der Aufstellung weiterer Maßnahmenkataloge zu unterscheiden. Bei den Beratungen wurde abschließend festgestellt, dass die Strategie als ausreichend robustes Instrument anzusehen ist, das vorbehaltlich einiger Aktualisierungen bestätigt werden sollte. Was jedoch die Umsetzung der Strategie mithilfe von Maßnahmenkatalogen anbelangt, so verlangten die Delegationen ein stärkeres Engagement der beteiligten Akteure und eine Fokussierung auf praktische Ergebnisse sowie auf operative und Koordinierungsaspekte.
5. Daher hat der Vorsitz vorgeschlagen, Schlussfolgerungen des Rates zu einer aktualisierten Strategie für das Informationsmanagement (IMS) für die innere Sicherheit in der Union zu erstellen, die den in diesem Bereich in den letzten fünf Jahren geleisteten Arbeiten Rechnung tragen.
6. Die Gruppe "Informationsaustausch und Datenschutz" hat den Vorschlag geprüft und sich in ihrer Sitzung vom 19. November 2014 auf den Entwurf der Schlussfolgerungen des Rates geeinigt, wobei die britische Delegation einen Vorbehalt eingelegt hat. Dieser Vorbehalt ist am 24. November 2014 zurückgezogen worden.
7. Der AStV wird daher gebeten, den Rat zu ersuchen, er möge den in der Anlage enthaltenen Entwurf von Schlussfolgerungen des Rates zu einer aktualisierten Strategie für das Informationsmanagement für die innere Sicherheit in der EU billigen.

² Dok. 13032/14 JAI 663 DAPIX 111 CRIMORG 76 ENFOPOL 260.

ENTWURF VON SCHLUSSFOLGERUNGEN DES RATES

**ZU EINER AKTUALISIERTEN STRATEGIE FÜR DAS
INFORMATIONSMANAGEMENT (IMS)**

FÜR DIE INNERE SICHERHEIT IN DER EU

DER RAT DER EUROPÄISCHEN UNION –

UNTER HINWEIS AUF

- das Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union ³, insbesondere Abschnitt 2.1, der eine Verbesserung des Informationsaustauschs zur Verbrechensbekämpfung fordert, hat für den grenzüberschreitenden Informationsaustausch den Grundsatz der Verfügbarkeit eingeführt und festgelegt, dass in Bezug auf "die Methoden für den Informationsaustausch" "die neuen Technologien in vollem Umfang genutzt werden" sollten und "die Methoden (...) an jede Art von Informationen angepasst sein" müssen;
- den Umstand, dass der Europäische Rat im Stockholmer Programm das Erfordernis der Kohärenz und der Konsolidierung bei der Entwicklung von Informationsmanagement und -austausch anerkannt und den Rat ersucht hat, eine Strategie der Union für Informationsmanagement anzunehmen und umzusetzen, die Folgendes umfassen sollte: Entwicklung gemäß den Anforderungen der Praxis, eine solide Datenschutzregelung, die Interoperabilität von IT-Systemen und die Rationalisierung der verschiedenen Instrumente sowie umfassende Koordination, Konvergenz und Kohärenz;
- die Schlussfolgerungen des Europäischen Rates vom 26./27. Juni 2014 ⁴, insbesondere Kapitel I "Freiheit, Sicherheit und Recht"; dort heißt es wie folgt: "Bei der Bekämpfung von Kriminalität und Terrorismus sollte die Union die nationalen Behörden durch die Mobilisierung aller Instrumente der justiziellen und polizeilichen Zusammenarbeit – mit einer verstärkten Koordinierungsrolle für Europol und Eurojust – unterstützen, unter anderem durch (...) einen verbesserten grenzüberschreitenden Informationsaustausch, einschließlich der Informationen über Strafregister";

³ Dok. 16504/04 JAI 559.

⁴ Dok. EUCO 79/14 CO EUR 4 CONCL 2.

UNTER BERÜCKSICHTIGUNG

- der Schlussfolgerungen des Rates zur verstärkten Umsetzung der "Prümer Beschlüsse" nach Ablauf der Frist vom 26. August 2011 ⁵;
- der Schlussfolgerungen des Rates zur Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates ("schwedischer Rahmenbeschluss") ⁶;
- der Schlussfolgerungen des Rates über einen noch effizienteren grenzüberschreitenden Austausch strafverfolgungsrelevanter Informationen ⁷;
- der Mitteilung der Europäischen Kommission vom 7. Dezember 2012 über das Europäische Modell für den Informationsaustausch '(EIXM) und die diesbezüglichen Schlussfolgerungen des Rates ⁸, insbesondere hinsichtlich der Aufgabe, die Automatisierung der bestehenden Verfahren für den Datenaustausch im Rahmen der Strategie für das Informationsmanagement (IMS) weiter zu erörtern;

UNTER HERVORHEBUNG DESSEN,

- dass das strategische Ziel der künftigen erneuerten EU-Strategie der inneren Sicherheit (ISS), bei der Bekämpfung der transnationalen Kriminalität und des transnationalen Terrorismus einen umfassenden und kohärenten Ansatz – insbesondere durch den Zugang zu sowie die Verfügbarkeit und den Austausch von Informationen – zu verstärken, durch Weiterverfolgung des Ziels einer Interoperabilität der Systeme und durch Verbesserung und Vereinfachung der bestehenden Werkzeuge für den Informationsaustausch bei der grenzüberschreitenden Strafverfolgung unter Einhaltung der bestehenden Datenschutzvorschriften gefördert wird;

⁵ Dok. 17762/11 JAI 892 DAPIX 163 CRIMORG 233 ENFOPOL 441 ENFOCUSTOM 160.

⁶ Dok. 15277/11 JAI 714 DAPIX 129 CRIMORG 176 ENFOPOL 346 ENFOCUSTOM 115 COMIX 719

⁷ Dok. 10333/12 JAI 356 DAPIX 65 CRIMORG 57 ENFOCUSTOM 43 ENFOPOL 147.

⁸ Dok. 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146.

UNTER BERÜCKSICHTIGUNG DESSEN,

- dass die Schlussfolgerungen des Rates zu einer Strategie für das Informationsmanagement (IMS) im Bereich der inneren Sicherheit in der EU ⁹ vom Rat unter der Voraussetzung gebilligt wurden, dass die Strategie langfristig angelegt ist und weiterentwickelt und ergänzt werden könnte und daher bis Ende 2014 überprüft werden sollte;
- dass die Strategie bisher durch drei Maßnahmenkataloge, jeweils mit einer Laufzeit von 18 Monaten, ergänzt wurde, in denen die konkreten Ziele, Verfahren, Aufgaben und Fristen festgelegt sind,
- dass die Strategie als ausreichend robustes Instrument anzusehen war, das vorbehaltlich einiger Aktualisierungen bestätigt werden sollte;
- dass in Anbetracht der im zweiten Zwischenbericht zur Umsetzung der IMS-Aktionspläne ¹⁰ dargelegten Zielsetzungen und Ergebnisse zur weiteren Umsetzung der Strategie ein stärkeres Engagement der auf nationaler Ebene wie auf der Ebene der EU beteiligten Akteure und eine Fokussierung auf praktische Ergebnisse sowie auf operative und Koordinierungsaspekte erforderlich sind;
- dass die EU-Agentur für IT-Großsysteme (eu-LISA) am 1. Dezember 2012 den Betrieb aufgenommen hat mit dem Ziel, tragfähige, langfristig angelegte Lösungen für das Management von IT-Großsystemen bereitzustellen und sich schrittweise zu einem Kompetenzzentrum weiterzuentwickeln;
- dass das Volumen des grenzübergreifenden Informationsaustauschs in den vergangenen Jahren zugenommen hat und die Mitgliedstaaten erwarten, dass sich diese Tendenz fortsetzen wird, was mit dem effizienten Einsatz moderner Technologien, z. B. der Automatisierung, sowie durch die Straffung der Routineverfahren und der Arbeitsabläufe, aufgefangen werden könnte;

⁹ Dok. 16637/09 JAI 873 CATS 131 ASIM 137 JUSTCIV 249 JURINFO 145.

¹⁰ Dok. 13032/14 JAI 663 DAPIX 111 CRIMORG 76 ENFOPOL 260.

IN DEM BEWUSSTSEIN, DASS

- ein effizienter und sicherer grenzüberschreitender Informationsaustausch ¹¹ die Grundvoraussetzung für die Verwirklichung der Ziele für den Bereich der inneren Sicherheit in der Europäischen Union ist;
- die Aufgaben der inneren Sicherheit je nach den nationalen Strukturen, Zuständigkeiten und rechtlichen Rahmenbedingungen auf eine ganze Reihe von Behörden (die "Praxis"-Seite) aufgeteilt sind und diese Aufteilung von Mitgliedstaat zu Mitgliedstaat variiert;
- das sektorübergreifende Informationsmanagement den disziplinübergreifenden Ansatz bereitstellt, der zum Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts benötigt wird; insbesondere bietet sie die Möglichkeit zu einem verstärkten Informationsaustausch und einer engeren Zusammenarbeit zwischen allen Beteiligten, damit die Bekämpfung der grenzüberschreitenden Kriminalität noch effizienter gestaltet werden kann;
- in Anbetracht der Bandbreite der bestehenden Instrumente für den grenzübergreifenden Informationsaustausch die Mitgliedstaaten verschiedentlich zum Ausdruck gebracht haben, dass es notwendig ist, für Kohärenz und Konsolidierung zu sorgen, und dass erst die bestehenden Instrumente und Vereinbarungen umgesetzt werden müssen, bevor neue Initiativen ergriffen werden;
- das Erfordernis eines kohärenten und wirksamen grenzübergreifenden Ansatzes durch die zunehmende Mobilität der Bürger, die immer vielschichtiger werdende Kriminalität und die infolgedessen auch immer vielschichtiger werdenden Kriminalitätsbekämpfungsstrategien der EU sowie dadurch immer dringlicher wird, dass die EU und die Mitgliedstaaten ihre Ressourcen optimal einsetzen müssen;
- die Bürger verlangen eine angemessene Abgewogenheit zwischen der Achtung ihrer Privatsphäre und ihren Sicherheitserwartungen.

¹¹ *In diesem Zusammenhang bezeichnet der Begriff "Information" alle Informationen oder Erkenntnisse, die die zuständigen Behörden der Mitgliedstaaten benötigen und die ihnen nach dem einschlägigen Rechtsrahmen zur Verfügung stehen, um das Ziel einer Verbesserung der inneren Sicherheit in der Union im Interesse der Unionsbürger zu erreichen.*

UNTER BETONUNG DESSEN, DASS

- mit der Strategie eine Richtschnur für die Gewährleistung eines Informationsaustauschs gegeben werden soll, bei dem sowohl dem Bedarf der Praxis als auch den Rechten des Einzelnen Rechnung getragen wird;
- mit der Strategie die Grundvoraussetzungen für eine fachgerechte, praxisorientierte und kosteneffiziente Entwicklung und Verwaltung von IT-Systemen festgelegt werden sollen;
- die Strategie den Weg hin zu einem strukturierten Informationsaustausch aufzeigt und die Grundlage für eine verbesserte Entscheidungsfindung und Steuerung bildet;

UNTER BEGRÜSSUNG UND BEFÜRWORDUNG

- der Arbeiten an den technischen Modalitäten für den grenzübergreifenden Informationsaustausch und insbesondere der Fortschritte in Bezug auf das universelle Nachrichtenformat (UMF) für einen verstärkten strukturierten Informationsaustausch über Grenzen hinweg und
- der Weiterentwicklung des universellen Nachrichtenformats (UMF) als einer der Kernkomponenten der Informationsaustauscharchitektur der EU gemäß den Schlussfolgerungen der UMF-2-Schlusskonferenz¹²;
- der laufenden Arbeiten an der Interoperabilität und erweiterten Synergie der Systeme sowie an der Automatisierung des Informationsaustauschs –

FASST DEN ENTSCHLUSS,

die Strategie für das Informationsmanagement (IMS) zu bestätigen und weiter mit dem Ziel durchzuführen, ein Informationsmanagement zu unterstützen, zu straffen und zu erleichtern, das

- a) auf folgenden Grundsätzen beruht:

¹² Dok. 10158/14 DAPIX 69.

- Das Informationsmanagement im Raum der Freiheit, der Sicherheit und des Rechts stellt ein wesentliches Instrument für die Umsetzung des Ziels einer Verbesserung der inneren Sicherheit in der Union und des Schutzes der Unionsbürger dar;
 - bei dem grenzübergreifenden Informationsaustausch im Bereich der Strafverfolgung ist ein ausgewogenes Verhältnis zwischen den Erfordernissen der Praxis und der Wahrung der Grundrechte zu wahren;
 - die für Informationsmanagement und -austausch vorgegebenen Prioritäten müssen den politischen, strategischen und operativen Prioritäten entsprechen und die Prioritäten der Praxis in Bezug darauf, wie die vorgenannten Ziele umgesetzt werden sollen, unterstützen;
 - Datenschutz, Datensicherheit und Datenqualität sind stets zu beachten;
 - Entwicklung und Verwaltung von IT-Systemen müssen fachgerecht, praxisorientiert und kosteneffizient erfolgen;
 - das Informationsmanagement muss funktionsorientiert sein, d.h. im Gegensatz zu einem zuständigkeits- oder organisationsorientierten System von den zu bewältigenden Aufgaben abhängen;
 - das Informationsmanagement muss den disziplinübergreifenden Ansatz bereitstellen, der zum Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts benötigt wird;
- b) aus Schwerpunktbereichen besteht, die in die nachstehenden Rubriken untergliedert sind und im Anhang näher erläutert werden:

I. Bedarf und Anforderungen

- Bedarf, Anforderungen und Mehrwert werden als Grundvoraussetzung für die Entwicklung bewertet.
- Die Entwicklung folgt vereinbarten Arbeitsabläufen im Bereich der Strafverfolgung und Modellen zur Gewinnung strafrechtlicher Erkenntnisse.
- Die Entwicklung unterstützt sowohl die datenschutzrechtlichen Anforderungen als auch den praktischen operativen Bedarf.

II. Interoperabilität und Kosteneffizienz

- Interoperabilität und Koordinierung werden sowohl in Bezug auf praktische Arbeitsabläufe als auch für technische Lösungen gewährleistet.
- Wiederverwendung ist die Regel.

III. Entscheidungs- und Entwicklungsprozesse

- Die Mitgliedstaaten werden von Anfang an in den Prozess eingebunden.
- Für jeden Teil des Prozesses gibt es eine eindeutige Zuständigkeit, wodurch Kompetenz, Qualität und Effizienz sichergestellt werden.

IV. Multidisziplinärer Ansatz

- Die interdisziplinäre Koordinierung im JI-Bereich wird sichergestellt.

Es werden die nötigen Schritte eingeleitet, um künftige detaillierte Aktionspläne mit realistischen Zeitvorstellungen und Fokussierung auf praktische Ergebnisse im Hinblick auf die Erfüllung der allgemeinen Zielsetzungen und Vorgaben dieser Strategie auszuarbeiten und erforderlichenfalls zu aktualisieren;

ERSUCHT

- die Vorbereitungsgremien des Rates, die sich mit Fragen des Informationsaustauschs und der Entwicklung von IT-Systemen befassen, die Strategie weiter umzusetzen;
- Beamte der Union und Vertreter der Mitgliedstaaten sowie Experten in den Gremien und Einrichtungen der Union, bei der Ausarbeitung von Entscheidungen, die unter anderem den Informationsaustausch auf bilateraler und regionaler Ebene und mit Drittstaaten oder Organisationen betreffen, der Strategie Rechnung zu tragen und sie ferner bei der Entwicklung und Durchführung von Programmen und Projekten für den Informationsaustausch und die Entwicklung von IT-Systemen zu berücksichtigen;
- die Mitgliedstaaten, die auf Unionsebene unternommenen gemeinsamen Bemühungen dadurch zu unterstützen, dass die Strategie auf nationaler Ebene als Leitlinie für politische und sonstige Entscheidungsträger in den zuständigen Behörden herangezogen wird, wenn es um Fragen des internationalen Informationsaustauschs und der Entwicklung von IT-Systemen (auch das "National Housekeeping" sowie um die Beziehungen zu Drittstaaten oder -organisationen) geht oder diese eine Rolle spielen;
- die Kommission, die in diesen Schlussfolgerungen vereinbarte Methodik bei der weiteren Ausarbeitung des europäischen Modells für den Informationsaustausch (EIXM) anzuwenden und für angemessene Finanzmittel für die zur weiteren Durchführung dieser Strategie erforderlichen Maßnahmen zu sorgen;
- die Kommission, die Möglichkeit einer Konsolidierung und Steigerung der Effizienz der bestehenden Rechtsvorschriften für den Informationsaustausch im Bereich der Strafverfolgung zu prüfen.

I. BEDARF UND ANFORDERUNGEN

1. Bedarf, Anforderungen und Mehrwert werden als Voraussetzung für die Entwicklung bewertet.

Dieser Schwerpunktbereich sieht vor, dass vor Einführung eines neuen Informationsaustauschs jeweils der damit verbundene Mehrwert zu bewerten ist. Ferner gelangt das Konzept der Verfügbarkeit der Information, das sich auf Zweck, Notwendigkeit und Verhältnismäßigkeit stützt, zur Anwendung.

Es wird eine obligatorische Bewertung des Praxisbedarfs sowie der praktischen und gesetzlichen Anforderungen für die betreffende Zusammenarbeit erfolgen, auch eine Bewertung der Frage, wie die Lösungen angewandt werden und wie nützlich sie sind, um die effektive operative Zusammenarbeit und die entsprechenden Arbeitsmethoden zu verbessern.

Daher wird sich die Entwicklung auf den Bedarf und die Anforderungen der einbezogenen Behörden stützen und an ihnen orientieren. Eine Bewertung der Nützlichkeit (einschließlich einer Kosten-Nutzen-Analyse) wird auch dazu beitragen, Prioritäten für die Entwicklung festzusetzen.

Das bedeutet Folgendes:

Wenn Initiativen betreffend den Informationsaustausch oder technische Lösungen auf die Agenda gesetzt werden, sind die Endnutzer und die Managementebene in den einzelnen Bereichen einzu beziehen. Ohne ihre Unterstützung können Bedeutung und Wert einer Initiative nicht beurteilt werden. Ihre Einbeziehung ist darüber hinaus wichtig, wenn es darum geht, für Ausgewogenheit zwischen Datenschutz und Praxisbedarf zu sorgen;

Überlegungen oder Erörterungen zu technischen Lösungen sind an der Bedarfs- und Anforderungsanalyse auszurichten;

Beratungen über Rechtssetzungsakte und/oder Vorstudien für technische Lösungen sollten nicht aufgenommen werden, bevor nicht die Praxisanforderungen ermittelt und dokumentiert wurden; jede Initiative im Bereich des Informationsaustauschs muss auf einer eingehenden Analyse der auf EU-Ebene und in den Mitgliedstaaten vorhandenen Lösungen, auf der Festlegung von Bedarf, Anforderungen und Mehrwert sowie auf der Bewertung der rechtlichen, technischen und finanziellen Auswirkungen der neuen Initiative beruhen;

es sollten eindeutige Bewertungskriterien entwickelt werden, die an systematische Evaluierungsprogramme gekoppelt sind;

die Bewertung der Frage, ob es zweckmäßig ist, beispielsweise bestimmte Informationsarten weiterzuentwickeln, sollte sich aus einem Prozess der Bestimmung strategischer Prioritäten ableiten.

2. Die Entwicklung folgt vereinbarten Arbeitsabläufen und Modellen zur Gewinnung strafrechtlicher Erkenntnisse

Die Verbesserung des Informationsaustauschs hängt in sehr starkem Maße davon ab, inwieweit dieser durch IT-Lösungen unterstützt wird. Um den Informationsaustausch zu fördern, muss die Informationstechnologie die Arbeitsabläufe im Rahmen der internationalen Zusammenarbeit im Bereich der Strafverfolgung unterstützen.

Die Arbeitsabläufe müssen einen raschen, effizienten, nutzerfreundlichen und kostenwirksamen Austausch von Informationen und strafrechtlichen Erkenntnissen ermöglichen. Zu diesem Zweck müssen die einzelnen Arbeitsschritte genau beschrieben, bekannt und zugänglich sein. Sie sollten fester Bestandteil der Systementwicklung und -beschaffung sein. Dadurch werden Management und Dokumentation der Entwicklung verbessert, und die Entwicklung wird durch den Bedarf der internationalen Zusammenarbeit im Bereich der Strafverfolgung gesteuert.

Das bedeutet Folgendes:

Die Arbeit an dem derzeitigen Konzept der gemeinsamen Anforderungen (Common Requirements Vision, CRV) sollte durch zusammen mit bzw. von den nationalen Behörden vorgenommene Analysen wesentlicher Anforderungen ergänzt werden; eine "Informations-Landkarte" (information map) sollte kontinuierlich einen Überblick über die Arbeitsabläufe und die entsprechenden Informationsflüsse der internationalen Zusammenarbeit ermöglichen, damit auf dieser Grundlage die Schnittstellen ermittelt werden können, an denen eine Harmonisierung erforderlich ist.

3. Die Entwicklung stützt sowohl die datenschutzrechtlichen Anforderungen als auch den praktischen operativen Bedarf

Die Zusammenarbeit zur Gewährleistung der inneren Sicherheit in der Union stellt hohe Anforderungen an den Datenschutz und an die Datensicherheit/einschließlich der Datensicherheit. So sind sowohl der Schutz der Privatsphäre als auch die Sicherheit der Arbeitsabläufe sicherzustellen, während für den Bedarf der Praxis die Nutzung und der Austausch von Informationen ermöglicht werden muss.

Ein hohes Maß an Sicherheit wird zugleich die Belange der Praxis und das Privatleben der Bürger schützen, ohne dass die Verfügbarkeit von Informationen beeinträchtigt wird, so dass den berechtigten Nutzern in nachprüfbarer Weise korrekte Informationen bei Bedarf zur Verfügung stehen, wenn dies nach den geltenden Rechtsvorschriften zulässig ist. Durch die angemessene Nutzung moderner Technologien, aber auch die Anpassung der Arbeitsabläufe und Maßnahmen zur Umsetzung des Datenschutzes wird dieses erleichtert. Ein verstärktes Vertrauen in diesen Bereichen zwischen den zuständigen Behörden ist ein wichtiger Schritt hin zu einer standardmäßigen gemeinsamen Nutzung von Daten.

Das bedeutet Folgendes:

Die gesetzlichen Anforderungen an den Schutz personenbezogener Daten und an Sicherheitsstandards müssen zusammen mit dem Bedarf der Praxis an Nutzung und Austausch von Informationen bewertet werden, damit für den Informationsaustausch und für die IT-Systeme das korrekte Maß an praxisbezogenen und technischen Sicherheitsstandards gewährleistet wird;

die Sammlung von Daten muss gezielt erfolgen, damit die Privatsphäre des Einzelnen geschützt, eine Informationsüberflutung der zuständigen Behörden verhindert und eine effiziente Kontrolle der Informationen erleichtert wird;

die Datensicherheit ist eine Grundvoraussetzung für den Datenschutz und muss durch organisatorische und technische Maßnahmen gewährleistet werden;

die verschiedenen Instrumente müssen im Interesse einer Arbeitserleichterung für die zuständigen Behörden gestrafft werden, wodurch das Schadensrisiko möglichst gering gehalten wird, ebenso wie durch eine Schulung betreffend die zur Verfügung stehenden Instrumente und deren Nutzung;

angemessene Maßnahmen zur Umsetzung des Datenschutzes müssen sachgemäße und regelmäßige operationelle Kontrollen vorsehen und sicherstellen, dass bei Verstößen angemessene Strafen auch wirklich zur Anwendung kommen;

zur Bewertung der Qualität und der Auswirkungen von Datenschutzmaßnahmen sollten systematische Evaluierungs- und Überwachungsverfahren entwickelt werden.

II. INTEROPERABILITÄT UND KOSTENEFFIZIENZ

4. Interoperabilität und Koordinierung werden sowohl in Bezug auf praktische Arbeitsabläufe als auch für technische Lösungen gewährleistet

Die Interoperabilität betrifft vielerlei Ebenen, wie etwa die gesetzliche, die inhaltliche, die praktische und die technische Ebene. Sie ist die Voraussetzung für einen effizienten Informationsaustausch und erleichtert diesen zugleich. Interoperable Lösungen und Kapazitäten gründen sich auf Initiativen und Vorschläge, die ihrerseits vom Bedarf und von den Anforderungen der Praxis ausgehen.

Technisch sollten IT-Lösungen und ihre Komponenten gemeinsam vereinbarten Standards und Grundsätzen entsprechen. Es sollten Standardlösungen angewandt und auf ein Mindestmaß beschränkt werden.

Ihre Anwendung wird für eine größere Kohärenz bei der Entwicklung und Verwaltung von Lösungen sorgen.

Sie wird auch die Interoperabilität und Koordinierung zwischen Systemen fördern. Daher werden bestehende Lösungen besser und stärker genutzt werden; so können die IT-Systeme größere Teile der Arbeitsabläufe unterstützen. Die Notwendigkeit einer doppelten Speicherung und doppelten Registrierung wird abnehmen und die IT-Unterstützung wird benutzerfreundlicher werden. Durch die Anwendung von gemeinsam vereinbarten Standards kann der Informationsaustausch von mehreren Zulieferern statt nur von einem Zulieferer unterstützt werden, so dass die Abhängigkeit von speziellen Zulieferern auf ein Mindestmaß reduziert wird. Langfristig werden dadurch auch die Anpassungskosten in den Mitgliedstaaten gesenkt.

Das bedeutet Folgendes:

Die "Informations-Landkarte" sollte einen vergleichenden Überblick über die Rechtslage auf Ebene der Union und der Mitgliedstaaten im Bereich des Informationsaustauschs enthalten;

die [vorgeschlagene]europäische Interoperabilitätsstrategie sollte durchgeführt werden; bestehende, gemeinsam vereinbarte Akkreditierungs-/Standardisierungsfunktionen sollten verwendet werden;

Möglichkeiten zur Systemintegration, wie z.B. Standardtechnologien und -fähigkeiten, die die Systemintegration erleichtern und darauf abzielen, Sicherheit, Skalierbarkeit und Leistung zu gewährleisten, sollten ermittelt werden;

Datenschutzmaßnahmen sollten sowohl auf Unions- als auch auf nationaler Ebene sowie zwischen beiden Ebenen koordiniert werden.

5. Wiederverwendung ist die Regel

Die Entwicklung ist mit hohen Kosten und erheblichen Investitionen verbunden, aber auch mit langfristigen Kosten für Verwaltung, Wartung und Support. Normalerweise fließt lediglich ein kleiner Teil der Gesamtkosten in die Entwicklungsphase. Dies ist nicht nur für die technische Entwicklung von Bedeutung, sondern auch im Hinblick darauf, dass keine neuen Rechtsgrundlagen oder praktischen Modalitäten festgelegt werden, wenn bestehende Rechtsgrundlagen oder Modalitäten genutzt bzw. erweitert werden können.

Daher muss die gemeinsame Nutzung und Wiederverwendung von nachhaltigen Lösungen eine Priorität in Bezug auf die Entwicklung und technische Verbesserungen darstellen. Die Wiederverwendung trägt dazu bei, dass Parallellösungen vermieden und bestehende Instrumente und Systeme, auch hinsichtlich ihrer Integration und Zweckmäßigkeit, weiterentwickelt werden. Infolgedessen werden frühere Investitionen verstärkt genutzt werden und wird ein geringerer Bedarf an neuen Investitionen bestehen. Je mehr Komponenten zur Verfügung stehen, desto weniger Zeit wird für die Entwicklung erforderlich sein.

Für eine effiziente Wiederverwendung ist eine "Informations-Landkarte", die einen Überblick über die bestehenden Informationsströme, -funktionen und -komponenten bietet, Voraussetzung. Die effiziente (Wieder-)Verwendung von erfolgreichen Lösungen erfordert außerdem einen konstanten Evaluierungsprozess und ein Beobachtungsinstrument, damit festgestellt werden kann, wie der Informationsaustausch funktioniert.

Das bedeutet Folgendes:

Die "Informations-Landkarte" sollte Informationsströme, -funktionen und -lösungen einbeziehen; ein pragmatischer, sachbezogener und ressourceneffizienter Evaluierungsmechanismus muss geschaffen werden. er sollte nicht auf bestimmte (Rechts-)Instrumente beschränkt sein, und es sollte sichergestellt werden, dass Erfahrungswerte aus früheren Evaluierungen genutzt werden können; zur Beurteilung der Wirkung ihrer Tätigkeit muss die Union Instrumente schaffen, um nicht nur die kriminellen Aktivitäten messen zu können, sondern auch die Wirksamkeit ihrer Anstrengungen zur Bekämpfung der Kriminalität; unter Berücksichtigung von Verfahren, die nicht nur aus der Union, sondern auch aus Drittländern stammen, sollte ein Modell für die gemeinsame Nutzung und Wiedernutzung nachhaltiger Lösungen ausgearbeitet werden; bestehende Instrumente, die für den Informationsaustausch genutzt werden, sollten eingehend auf ihre Effizienz und Wirksamkeit hin überprüft werden, damit sie gestrafft werden können – auf jeden Fall, bevor damit begonnen wird, neue Instrumente zu entwickeln.

III. ENTSCHEIDUNGS- UND ENTWICKLUNGSPROZESSE

6. Die Mitgliedstaaten werden von Anfang an in den Prozess eingebunden

Entscheidungen auf Unionsebene über Zusammenarbeit, Informationsaustausch und Entwicklung von IT-Systemen haben erhebliche Auswirkungen – und zwar sowohl kurzfristig als auch aus einer "Lebenszyklus"-Perspektive – auf die Arbeitsabläufe, Strukturen, Investitionen und Haushalte der Mitgliedstaaten. Ein voll funktionsfähiges Endergebnis erfordert intensive Koordinierung auf nationaler Ebene sowie Gegenseitigkeit und Zusammenwirken zwischen der nationalen und der Unionsebene.

Die Behörden der Mitgliedstaaten, die für die nationale Umsetzung von Arbeitsabläufen, Methoden und Entwicklungen zuständig sind, müssen bereits vom Beginn der Entwicklungsprozesse auf europäischer Ebene an eingebunden werden. Um einen umfassenden Beitrag leisten zu können, sollten die Mitgliedstaaten, sowohl was die Arbeitsabläufe als auch was die Technik betrifft, im eigenen Bereich für Interoperabilität sorgen und ihre eigenen Entwicklungsprozesse festlegen.

Das bedeutet Folgendes:

Die Informationsmanagementstrategien oder -maßnahmen auf nationaler und auf Unionsebene sollten miteinander im Einklang stehen;

Endnutzer und maßgebliche Interessenvertreter sollten sowohl auf nationaler als auch auf Unionsebene einbezogen werden;

die Behörden in den Mitgliedstaaten müssen ihre eigenen Entwicklungsprozesse ermitteln und gestalten.

7. Für jeden Teil des Prozesses gibt es eine eindeutige Zuständigkeit, wodurch Kompetenz, Qualität und Effizienz sichergestellt werden

Um den Entwicklungsprozess besser steuern zu können, müssen die Rollen und Zuständigkeiten der einzelnen Akteure eindeutig festgelegt werden. In verschiedenen Bereichen, wie z.B. Aufgabenstruktur und Systemarchitektur ("business and technical architecture"), Methoden und Modelle, Management, Finanzen und Kontrolle, sind besondere Zuständigkeiten erforderlich. Beratungen über (technische) Lösungen müssen auf Ebene der geeigneten systemtechnischen und -architektonischen Zuständigkeiten erfolgen. Entscheidungen auf der Managementebene oder der politischen Ebene müssen auf die für diese Ebene geeigneten Themen abstellen.

So werden die Rollen ermittelt, die Zuständigkeiten festgelegt und die Strukturen geschaffen werden müssen, um sicherzustellen, dass alle betroffenen Parteien auf der richtigen Ebene und in der richtigen Phase des Prozesses eingebunden werden, aber auch um sicherzustellen, dass insgesamt für Koordinierung und Kohärenz gesorgt ist.

Das bedeutet Folgendes:

Die Rollen und Zuständigkeiten auf den verschiedenen Ebenen (innerhalb der bestehenden oder geplanten nationalen Behörden und Organe, Einrichtungen und sonstige Stellen der Union usw.) müssen ermittelt und organisiert werden;

die Funktionen zur Vorbereitung der strategischen Entscheidungen betreffend Informationsmanagement und Entwicklung von IT-Systemen müssen ermittelt/festgelegt werden;

Funktionen für Verwaltung, Weiterentwicklung und Evaluierung von (praxisbezogenen und technischen) Lösungen müssen vorhanden sein.

IV. MULTIDISZIPLINÄRER ANSATZ

8. Die multidisziplinäre Koordinierung wird sichergestellt

Mit der derzeitigen Strategie für das Informationsmanagement soll die Verwaltung der Informationen unterstützt, gestrafft und erleichtert werden, die von den zuständigen Behörden benötigt werden, um die innere Sicherheit in der Union zu gewährleisten. In der Praxis wird es sich bei den betreffenden Behörden im wesentlichen um die mit Strafsachen befassten Strafverfolgungs- und Justizbehörden handeln, aber auch mit anderen Behörden und Quellen wird ein Informationsaustausch notwendig sein. Die Strategie für Informationsmanagement anerkennt und berücksichtigt den multidisziplinären Ansatz, der notwendig ist, um die obengenannten Ziele zu erreichen und – unabhängig von der im Besitz der Informationen befindlichen Stelle – die Weitergabe und Wiederverwendung von Informationen zu erleichtern. Die moderne Technologie gestattet es, das gewünschte Verfügbarkeitsniveau zu erreichen, das es seinerseits ermöglicht, Störungen und die manuelle Wiedereingabe auf ein Mindestmaß zu beschränken und die Qualität der Informationen zu verbessern. Dieselbe Technologie ermöglicht es, das Datenschutzniveau, einschließlich des Datensicherheitsniveaus, beizubehalten oder zu erhöhen.

Die Strategie zielt darauf ab, den Informationsaustausch zwischen den zuständigen Behörden in funktioneller und technischer Hinsicht zu erleichtern, wenn dieser gesetzlich vorgesehen ist. Daher erfordert die Strategie Mittel zur Gewährleistung der Interoperabilität und sieht derartige Mittel vor. Sie bewirkt selbst keine Vernetzung der unterschiedlichen Datenbanken und sieht auch keine speziellen Arten des Datenaustauschs vor, aber sie stellt sicher, dass – bei Vorliegen der operativen Anforderungen und einer Rechtsgrundlage – die einfachste, am leichtesten nachvollziehbare und kostenwirksamste Lösung gefunden wird.

Dies bedeutet, dass die Anstrengungen zur Verwirklichung der Interoperabilität ein Zusammenwirken zwischen allen zuständigen Behörden und Organisationen erfordern. Welche Behörden und Organisationen dies sind, wird sich nach dem jeweils zu deckenden Bedarf richten. Mit der in dieser Strategie dargelegten Methodik – insbesondere den Schwerpunktbereichen 1 bis 3 – wird dafür gesorgt, dass die Interoperabilität zwischen den unmittelbar für die innere Sicherheit der EU zuständigen Behörden und über diese Behörden hinaus gewährleistet wird, wann immer dies erforderlich und verhältnismäßig ist, wobei allerdings auch dafür gesorgt wird, dass die Interoperabilität auf diese Fälle beschränkt ist.

Das bedeutet Folgendes:

*Der Informationsaustausch darf nicht durch Fragen der Zuständigkeit behindert werden
(gegenseitige Anerkennung von verschiedenen nationalen Strukturen);*

*IT-Unterstützung und -Standardisierung (einschließlich Architekturgrundsätze und Informations-
/Datenmodelle) müssen so horizontal wie möglich angelegt sein und sich auf gemeinsame
Grundsätze und Koordinierung stützen;*

*Datenschutz- und Datensicherheitsmaßnahmen sollten zwischen der Ebene der Union und den
Mitgliedstaaten koordiniert werden;*

*im Rahmen dieses multidisziplinären Ansatzes sollte eine systemübergreifende Folgenabschätzung
berücksichtigt werden.*
